FedRAMP JAB P-ATO VULNERABILITY SCAN REQUIREMENTS GUIDE

Version 2.0

November 20, 2017

FedRAMP

DOCUMENT REVISION HISTORY

DATE	VERSION	PAGE(S)	DESCRIPTION	AUTHOR
5/27/2015	1.0	All	Initial Version	C. Andersen
6/6/2017	1.0	Cover	Updated logo	FedRAMP PMO
11/20/2017	2.0	All	Reformatted into new template	FedRAMP PMO

WHO SHOULD USE THIS DOCUMENT

This document is intended for the use by the following groups:

- Federal Risk and Authorization Management Program (FedRAMP) Cloud Service Providers (CSPs), to ensure they provide vulnerability scans as required.
- FedRAMP Information System Security Officers (ISSOs), to ensure the requirements are met and maintained.
- Leveraging agencies, to understand the scanning required by CSPs.

HOW TO CONTACT US

Questions about FedRAMP or this document should be directed to info@fedramp.gov.

For more information about FedRAMP, visit the website at http://www.fedramp.gov.

TABLE OF CONTENTS

1. PURPOSE

This guide describes the requirements for all vulnerability scans of FedRAMP Cloud Service Provider's (CSP) systems for Joint Authorization Board (JAB) Provisional Authorizations (P-ATOs).

2. CLOUD SERVICE PROVIDER REQUIREMENTS

CSPs are required to perform vulnerability scanning of their information systems monthly (at a minimum). Each CSP is responsible for the delivery of the results of these vulnerability scans to their authorization official in a timely manner. These vulnerability scans are the cornerstone for the continuous monitoring of a CSP's risk posture, enabling authorization officials to continue to authorize a CSP system for use.

Each CSP must identify and use vulnerability assessment tools within their security control implementations approved by the JAB through the P-ATO. These include:

- Operating system and network vulnerability scanners
- Database vulnerability scanners
- Web application vulnerability scanners

FedRAMP security authorization requirements specify that initial vulnerability scans for the P-ATO shall be performed by a Third Party Assessment Organization (3PAO), to provide independent validation of the scan results. CSPs must use the same tools for continuous monitoring as were used by the 3PAO for the P-ATO process. In some circumstances, CSPs may request changes to these tools. However, continued use of the previous tools must continue until all identified vulnerabilities from the original tools have been mitigated. The length of overlap is dependent on the CSP correcting the remaining vulnerabilities.

To ensure FedRAMP has all of the required information to perform the vulnerability analysis, the CSP must submit the following information:

- Vulnerability scan data
  - Raw scan files (native scanner files – usually some form of XML, CSV, or structured data format).
  - Exported summary reports (PDF, MS Word, or other readable documents). Summary reports should include Executive Summary, Detailed Summary, and Inventory Report. Actual reporting capabilities may vary by tool.
- Current and accurate system inventory. CSPs shall deliver a current system inventory identifying the components of the information system within the authorization boundary. The inventory must be complete and contain all boundary components.

The system inventory must be delivered in a machine-readable format (XLS, CSV, XML). It is critical that the vulnerability scans and the provided system inventory is machine matchable (IP addresses, system names, or other unique identifiers). Vulnerability scans and inventories that cannot be matched will by rejected by the PMO.

CSPs are also responsible for ensuring the highest quality vulnerability scans. Below is a list of requirements to ensure the quality of the scanning is acceptable for the FedRAMP program.

- **Authenticated/Credentialed Scans**: Vulnerability scans must be performed using system credentials that allow full access to the systems. Scanners must have the ability to perform in-depth vulnerability scanning of all systems (where applicable). Systems scanned without credentials provide limited or no results of the risks. All unauthenticated scans will be rejected unless an exception has been previously granted due to applicability or technical considerations.
- **Enable all Non-destructive Plug-ins**: To ensure all vulnerabilities are discovered, the scanner must be configured to scan for all non-destructive findings. Any vulnerability scans where plug-ins are limited or excluded will be rejected. Exceptions may occur based on specific requests from the government for re-scans or targeted scans. These scans must comply with the directions provided by the government.
- **Full System Boundary Scanning**: Each scan must include all components within the system boundary. Reduced number of components or missing categories will result in rejected scans. In some cases, sampling is acceptable; however this sampling must be approved as a part of the initial Security Assessment Plan for P-ATO, and approved as a part of the Continuous Monitoring Plan at the time of P-ATO. Sampling must include a complete and comprehensive representative sample of the information system components. This includes scanning multiple components of the same category in addition to scanning all component categories. (Note: sample scanning is approved based on the ability to prove the component categories are identically configured. These categories must be maintained through configuration management and all components must be similarly configured. Discovery of mis-configured items may result in the revocation of sampling and require future scans to be comprehensive, including all system components).
- **Scanner Signatures Up to Date:** CSPs must ensure that the vulnerability scanner used is up to date and includes the latest versions of the vulnerability signatures. Before scanning, each scanner must be updated to reflect the latest version of the scan engine as well as the signature files.
- **Provide Summary of Scanning:** Each scan submission must be accompanied by a summary of the scanning performed. The summary must include a listing of all the scan files submitted, which scanning tools were used, and a short summary of the purpose of the scan (e.g. monthly scans, re-scans, verification scans, etc.). In addition, the summary should discuss the configuration settings of the scanner,

including whether the signatures were limited for targeted, verification scans or if the scope of the scans excluded certain components or IP addresses. IP address ranges and/or a description of the targets are required.

- **"POA&M" All Findings:** Findings within the scans must be addressed in a Plan of Action and Milestones (POA&M) or other risk acceptance requests and maintained until the vulnerabilities have been remediated and validated. Additional details on the POA&M requirements can be found in the POA&M Template User Guide on FedRAMP.gov website.

3. FEDRAMP ACTIVITIES

FedRAMP evaluates all vulnerability scans submitted and provides a summary report to the JAB. In addition, agencies looking to leverage a CSP will also have access to the most recent risk posture information, including the continuous monitoring reports and POA&M.

FedRAMP CSPs can be complex and ever-changing. It is critical that FedRAMP maintain a current risk posture of the system through the scanning and continuous monitoring documentation. To accomplish this, FedRAMP utilizes automated tools for the evaluation, analysis, and reporting of the risk posture. The system ISSO will review the reports and make additional modifications or additions to ensure an accurate risk posture is presented in the summary reports.

4. REMEDIATION

Systems that fail to meet the quality or timeliness of the vulnerability scan submission requirements will be subject to actions. These actions may include one or more of the following:

- FedRAMP may require an immediate re-scan of the system. FedRAMP will clearly document the required adjustments necessary for the re-scan.
- FedRAMP may require a 3PAO to perform future scans for a period of time if the CSP is unable to meet the FedRAMP requirements.
- Continuous issues may result in FedRAMP requiring a Corrective Action Plan from a CSP as part of maintaining a P-ATO and communicating with known agencies the deficiencies with meeting scanning requirements.
- The FedRAMP JAB can also revoke a P-ATO for failure to meet these requirements and remove the vendor from the FedRAMP website.

FedRAMP reserves the right to take any of the actions listed above based on the severity of the deficiency.

APPENDIX A: FedRAMP ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page under Program Overview Documents.

(https://www.fedramp.gov/resources/documents-2016/)

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.